REMARKS

Claims 1-45 were presented for examination and were pending in this application. In an Office Action dated June 8, 2004, claims 1-28 and 30-45 were rejected; and claim 29 was objected to. Applicants hereby amend claims 2, 4, 19, 26, 30-35, 42 and 43. These claim amendments add no new matter. Applicants now request reconsideration and allowance of claims 1-45.

Applicants thank Examiner for examination of the claims pending in this application, and the below-summarized interview of October 4, 2004. Applicants address comments from the Office Action below.

I. Rejections Under § 102(e) – Shostack et al.

In paragraph 5 of the Office Action, Examiner rejects claims 1-5, 8-20, 23-28, 30, 33, 34 and 39-45 under 35 U.S.C. § 102(e) as being anticipated by Shostack et al. (U.S. Patent No. 6,298,445B1). Applicants respectfully traverse this rejection. During the interview, Applicants Attorneys (Brian Hoffman and Dorian Cartwright) argued that Shostack et al. failed to disclose a network-based identification of a version and/or patch level of the operating system and/or service on a remote host. As a result, Examiner and Applicants agreed that claim 44 was allowable and, further, that Shostack et al. failed to anticipate claim 1. Since claim 45 depends on claim 44, claim 45 is allowable for at least the same reasons as claim 44. Also, since claim 39 recites limitations of similar scope to claim 1; claims 40-41 depend on claim 39; and claims 2 and 3 depend on claim 1, each of these claims are patentable over Shostack et al. for at least the same reasons as claim 1.

Amended claims 4, 19, 26, 30, 33, 34 and 42, each recite a method of examining a network comprising, in relevant part, receiving a set of packets from a remote host (or remote equipment) and identifying conditions based on inferential information in the received packets. More specifically, claim 4 identifies a version of an operating system and a version of a service; claim 19 identifies an operating system and a service; claims 30 and 42 identify a vulnerability; claim 33 infers an unknown vulnerability; and claim 34 identifies a security policy violation. Advantageously, network-based examination of a host non-intrusively determines host conditions. Furthermore, network-based examination is more reliable by inferentially determining network conditions rather than

relying on easily compromised (e.g., by hackers) and insufficient (e.g., fail to identify version and/or patch level) self-identification techniques such as banners.

Moreover, amended claim 26 recites determining a version and patch level of an operating system and service, and amended claims 4 and 13 recite determining a version of an operating system and service. Advantageously, by determining a host's characteristics to these additional levels of granularity, the identification of vulnerabilities, among other things, is more accurate. In particular, vulnerabilities can be addressed in later versions or patches of software, and additional vulnerabilities can result from later versions or patches.

Shostack et al. generally discloses automatic enhancements to computer security software. The fourth application assesses the operating system of various computers and monitors the network for security vulnerabilities (Col. 7:20-24), but Shostack et al. does not disclose how to assess the operating system. While Shostack et al. discloses software enhancements based on newly discovered vulnerabilities (Col. 7:42-43), there is no disclosed method for determining these vulnerabilities. Shostack et al. also discloses a table of information contained in a security vulnerabilities database (Table 1). However, this table is used to provide solutions to security breaches (Col. 7:24-27), not to determine vulnerabilities.

Thus, Shostack et al. does not teach or suggest the invention as recited in claims 4, 19, 26, 30, 33, 34 and 42. In the claims, inferential information (e.g., in reflex packets) allows identification of network conditions listed above, whereas Shostack et al. fails to address how to assess an operating system and service. Furthermore, amended claims 4, 13 and 26 identify not only the operating system, but also the version, and claim 26 also identifies the patch level. Therefore, Applicants submit that claims 4, 19, 26, 30, 33, 34 and 42 are patentable over Shostack et al. Since claims 5-12 depend from claim 4; claims 14-18 depend from claim 13, claims 20-25 depend from claim 19; and claims 27-28 depend from claim 26, these claims are patentable over Shostack et al. for at least the same reasons.

Amended claim 43 recites, in relevant part, sending reflexive packets containing information according to an RFC protocol and indicative of an operating system and

service version and patch levels. Advantageously, there are thousands of RFC protocols to provide information indicative of host characteristics. Again, Shostack et al. fails to teach or suggest how to assess an operating system and and fails to address version and/or patch levels. Moreover, claim 43 provides a wide-spread baseline in RFC protocols for identifying host characteristics.

II. Rejections Under § 102(e) – Hill et al. and Diersch et al.

In paragraph 6 of the Office Action, Examiner rejects claims 31, 35, 36 and 38 under U.S.C. § 102(e) as being anticipated by Hill et al. (U.S. Patent No. 6,088,804). In paragraph 7 of the Office Action, Examiner rejects claim 32 under U.S.C. § 102(e) as being anticipated by Diersch et al. (U.S. Patent No. 6,101,606). Applicants respectfully traverse this rejection. In relevant part, the claims recite inferential information to allow network conditions. In particular, claim 31 identifies a trojan application; claim 32 identifies unauthorized software use; and claim 35 compares reflex signatures.

Hill et al. generally discloses a security system for responding to a security attack. Training signatures for simulated attacks are defined by a plurality of security events such as a Trojan horse (Col. 5:46-48; Col. 5:58-61). However, Hill et al. also fails to teach or suggest inferential information to determine recited network conditions. Instead, Hill et al. recognizes security events by apparently intercepting packets rather than causing reflex packets to be sent from the host.

Diersch et al. generally discloses a system for securing protected software against unauthorized use in computer networks. A program blocks further execution of protected programs when failing to establish a connection to an authorization component (Col. 5:24-31). Again, Diersch et al. fails to teach of suggest inferential information to identify unauthorized software use. Diersch et al. instead explicitly determines whether a protected program is authorized rather than causing reflex packets to be sent from the host.

III. Rejections Under § 103(a)

In paragraphs 8, 9 and 10 of the Office Action, Examiner rejects claims 6 and 22, 7 and 21, and 37, respectively under U.S.C. § 103(a) as being unpatentable over Shostack

et al. in combination with other references. Because these dependent claims have corresponding base claims that are patentable over Shostack et al., as discussed above, these claims are patentable over Shostack et al. for at least the same reasons.

IV. Objection

In paragraph 11 of the Office Action, Examiner objects to claim 29 as being dependent upon a rejected base claim, but indicates that it would be allowable if rewritten in independent form including all of the limitations of the base claim. However, since claim 29 depends from allowable base claim 26, such amendment is not necessary. Thus, Applicants have respectfully obviateted the objection.

CONCLUSION

In sum, Applicants respectfully submit that claims 1-45 as presented herein, are patentably distinguishable over the cited references either alone or in combination (including references cited, but not applied). Therefore, Applicants request reconsideration and allowance of these claims.

In addition, Applicants respectfully invite Examiner to contact Applicants' representative at the number provided below if Examiner believes it will help expedite furtherance of this application.

RESPECTFULLY SUBMITTED,

Date: August 8, 2004 By: Dorian Cartwright

Dorian Cartwright, Attorney of Record
Registration No. 53,853
FENWICK & WEST LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Phone: (650) 335-7247
Fax: (650) 938-5200